Remix GmbH
Hard- und Software
Wolfbachring 38 4665 Oftringen Tel. 079 6 477 457 Fax 062 797 06 00
www.remix-gmbh.ch

Allgemeine Informationen über ein Netzwerk

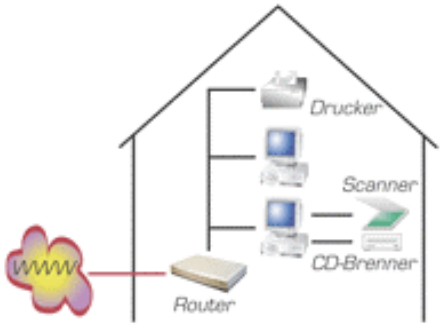
Um PC/Mac und Peripherie im Netzwerk nutzen zu können braucht es die erforderliche Verkabelung des Gebäudes. Die Gebäudeverkabelung sollte so ausgelegt werden dass die optimale Geschwindigkeit der Geräte genutzt werden können. Da es nicht immer möglich ist dies gewährleisten zu können, werden hier die häufigsten Möglichkeiten aufgezeigt.

Wir möchten Ihnen helfen alle wichtigen Kriterien zu beachten und Ihnen mit Rat und Tat zur Seite zu stehen.

Die Angabe über die beschriebenen Produkte basieren auf Zyxel Produkten. Unter Berücksichtigung wichtiger Kriterien können auch Alternativ-Produkte verwendet werden.

Die Gebäudeverkabelung

QoS: Qualitätsbedürfnisse im Netzwerk



Das Internet-Protokoll (IP) wurde als sogenanntes «Best-Effort»-Datenprotokoll entworfen. Es betrachtet daher Phänomene wie Jitter, Latency oder Datenverlust als unüberwindbare Hürde und bietet dafür keine technische Lösung. Bei der Definition des Basis-IP-Protokolls wurde dieses Problemfeld nicht berücksichtigt. Das Ergänzungsprotokoll IEEE 802.1p beschreibt die Datenpriorisierung (Quality-of-Service) in LANs und bietet die gewünschte Übertragungsqualität. Dazu müssen die notwendige Priorität und Bandbreite konfiguriert werden. Datenpakete z.B. für Echtzeitanwendungen (VoIP, Video-Streaming) werden mit einer Priorisierungsinformation versehen und entsprechend verarbeitet.

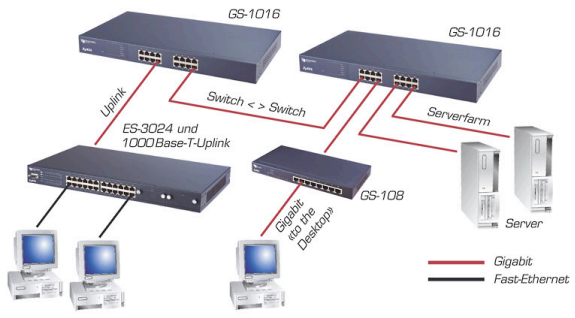
VLAN: Virtuelle Netzwerke

Ein virtuelles LAN ist eine Gruppe von Rechnern, die auf MAC-Ebene in einer autonomen, sicheren Domain (z.B. IP-Subnetz) zusammengefasst sind. Es findet daher kein Multicast- oder Broadcast-Verkehr ins VLAN hinein oder vom VLAN heraus statt. Die Zugehörigkeit zu einem VLAN hängt nicht von der geografischen Lage des Netzknotens ab. Sie ist ausschliesslich durch Software-Konfiguration bestimmt. Sie kann sehr schnell geändert werden, wenn ein Rechner einer neuen Arbeitsgruppe zugeordnet werden soll. Die Zuordnung der einzelnen Knoten (Rechner) findet dabei in einem VLAN-fähigen Switch statt. Unproblematisch ist diese Technik, solange nur ein LAN-Switch verwendet wird. Soll ein virtuelles Netz über mehrere Switches ausgedehnt werden, so sind die geführten MAC-Adressen um die Nummer des virtuellen Netzes zu ergänzen. Die so entstehenden Tabellen müssen über das ganze Netz konsistent gehalten werden. Gemanagte Dimension-Switches unterstützen den Netzinformationen-Austausch via GVRP (Global-Virtual-LAN-Routing-Protocol), ähnlich den Routern mit Routing-Protokollen.

VLAN-Konfigurationsvariante

Auto-Cross-over (Auto-MDI/MDIX)

Auto-MDI/MDIX ermöglicht die automatische Anpassung der Sende- und Empfangsleitung eines Ports, d. h. das angeschlossene Ethernet-Kabel (gekreuzt oder nicht gekreuzt) sowie die Konfiguration der Gegenstelle. Alle Auto-MDI/MDIX-Ports können so als Uplink-Port genutzt werden. Sämtliche 10/100-Mbps- und 1-Gbps-Ports der Dimension-Serie verfügen über dieses Feature.



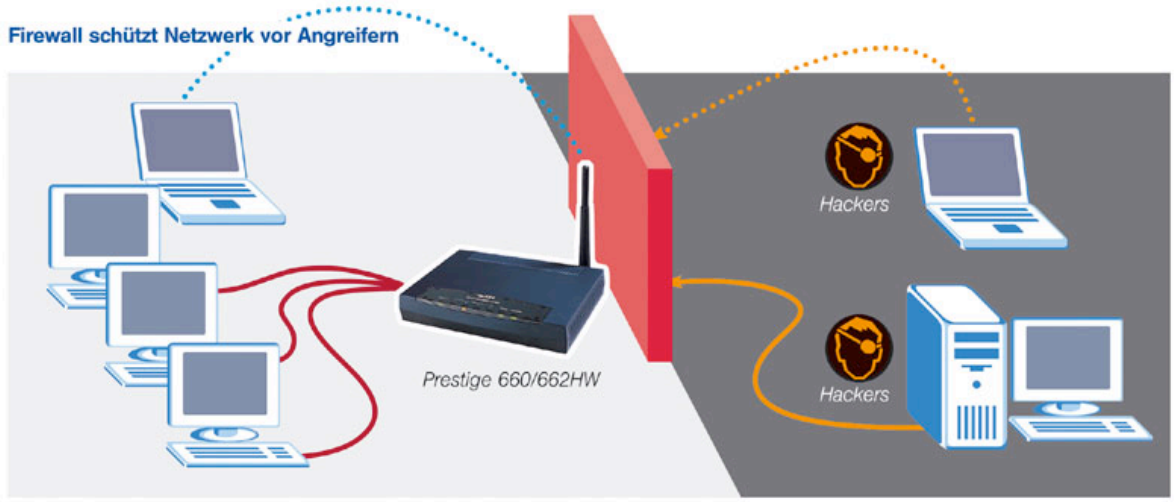
Mögliche Gigabit-Verbindungen

Schutz gegen aussen mit einer FireWall

Was kann eine Firewall?
Eine Firewall kontrolliert die Zugriffe auf ein Netzwerk und schützt vor Hacker-Angriffen. Hacker versuchen, über das Internet in ein Computersystem oder ein Netzwerk einzudringen, um Schwachstellen ausfindig zu machen resp. aufzuzeigen. Die Ziele eines Angriffes sind meist Daten zu stehlen, oder einen Schaden anzurichten. Einen zuverlässigen Schutz erwirbt man sich mit einer Firewall, die das Netzwerk mit unterschiedlichen Sicherheitstechnologien gegen unbefugte Zugriffe abschottet.

Unterschiedliche Firewall-Typen
Man unterscheidet zwischen Soft- und Hardware-Firewalls. Eine Hardware-Firewall ist punkto Installation und Unterhalt wesentlich einfacher zu administrieren und weniger problemanfällig bei Betriebssystem- und Software-Updates. Die Grösse einer Firewall bestimmt sich aufgrund der Anzahl PCs in einem Netzwerk.

Firewalls für alle Bedürfnisse
ZyXEL deckt mit der aktuellen ZyWALL-Serie alle Bedürfnisse vom Homeuser bis KMU ab. Alle Firewalls von ZyXEL enthalten die VPN-Funktionalität. Mit VPN ist es möglich, Daten geschützt zwischen zwei Standorten auszutauschen.

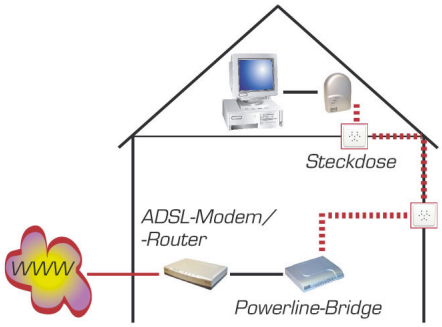


Mögliche Varianten für abgelegene Räume zu erschliessen

PowerLine

Was ist Powerline?

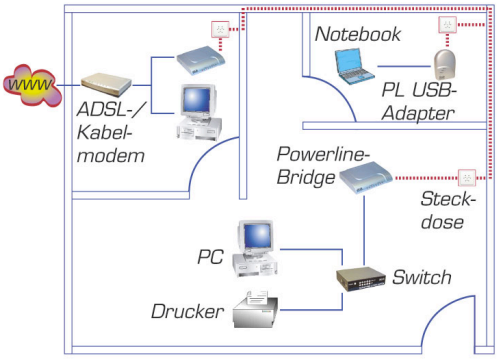
Mit der Powerline-Technologie wird die Datenübertragung auf dem hausinternen Stromnetz zur Realität. Die Technologie erreicht eine Geschwindigkeit von bis zu 14 Mbps und verwendet für die Übertragung das Mehrträgerverfahren OFDM (Orthogonal-Frequency-Division-Multiplexing). Der Übertragungskanal wird im Frequenzbereich 4,5 bis 21 MHz in viele voneinander unabhängige Teilkanäle unterteilt. Diese Powerline-Technologie ist auf die Übertragung in einer Wohnung oder einem Einfamilienhaus ausgelegt. Da fast jeder Raum in einem privaten Haushalt über eine Stromsteckdose verfügt, kann man ohne zusätzliche Verkabelung überall Powerline-Geräte einsetzen.



Powerline: Datenübermittlung über Strom

Einsatzgebiet

Praktisch jeder Raum verfügt über eine Stromsteckdose, dadurch können auch mehrere PCs mit Powerline über das Stromnetz verbunden werden. Sämtliche Verkabelungen entfallen. So kann man Powerline-Geräte einsetzen und z. B. das Büro im Keller einfach und schnell mit dem bestehenden Internetzugang im Erdgeschoss verbinden. Die Powerline-Geräte werden am Strom-netz und am PC angeschlossen. Dadurch werden Steckdosen im privaten Haushalt im Nu zum Internetzugang umfunktioniert.



Sicherheit

Die DES (56 bit)-Verschlüsselung bietet beste Sicherheit gegen Abhörversuche im Home-Networking. Dazu werden alle Powerline-Geräte, welche miteinander kommunizieren dürfen, mit demselben Passwort konfiguriert. Allen anderen Powerline-Geräten wird der Zugriff verweigert. Es empfiehlt sich das Standard-Netzwerk-Passwort mit der gelieferten Windows-Software zu ändern.

Reichweite

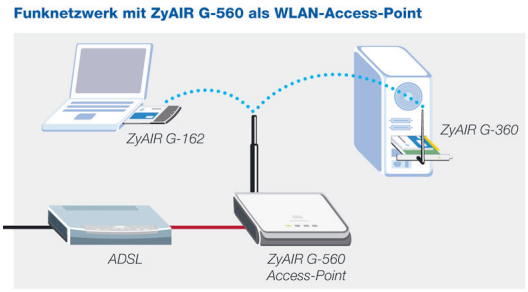
Bei optimalen Verhältnissen wird eine Reichweite von bis zu 300 Metern erreicht. Die Distanz ist stark abhängig von der Beschaffenheit des Stromnetzes. In privaten Haushalten ist ein Drehstromnetz mit drei verschiedenen getrennten Phasen vorhanden. Da die Technologie grundsätzlich phasenübergreifend funktioniert, ist die Funktion gewährleistet.

Störungen

Obwohl elektrische Geräte Stromschwankungen auf dem Netz verursachen, wird die Datenübertragung nicht gestört. Denn das bereits erwähnte Mehrträger-Modulationsverfahren gleicht diese Stromschwankungen aus und schafft sehr gut Abhilfe gegen die unterschiedlichsten Arten von Störungen.

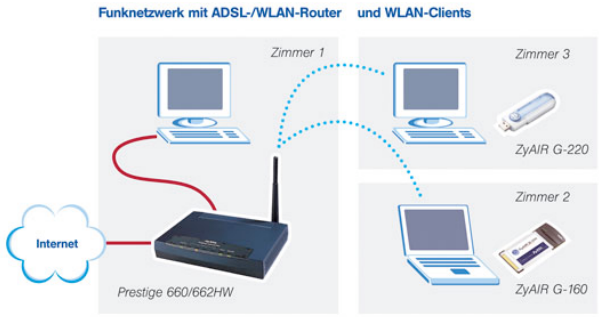
W-LAN

Wireless-LAN ? Datenübertragung über Funk



Mit Wireless-LAN werden Daten zwischen einzelnen PCs und/oder Netzwerken via Funk übermittelt. Beim Internetzugang wird ein Wireless-LAN-Access-Point installiert, an den übrigen Arbeitsplätzen je ein WLAN-Client-Adapter. Ohne teure Kabelinstallationen ist es so möglich, dass alle Computer drahtlos im Internet surfen. Der MAC-Adressfilter sowie die WEP-Verschlüsselung schützen das Netzwerk vor ungewollten Zugriffen. Mit der erweiterten Sicherheitsfunktion nach dem Standard IEEE 802.1x müssen sich die Clients mit einem persönlichen Benutzernamen und Passwort beim Access-Point anmelden. Wenn all diese Sicherheitsstufen sorgfältig angewendet werden, kann das Wireless-LAN auf einem recht hohen Sicherheitslevel betrieben werden.

Vorteil Funkverbindungen/"Access-Point"



Damit es zwischen mehreren PCs funkt, braucht es einen Access-Point, worüber die verschiedenen Clients kabellos auf Daten zugreifen können. Dank der Wi-Fi Kompatibilität (WiFi = Zertifikat für WLAN-Standards) können sich alle Wireless-Clients mit den folgenden (am meisten verbreiteten) Standards anmelden: 802.11b (11 Mbps), 802.11g (54 Mbps), 802.11g+ (125 Mbps). Mit dem Einsatz von externen Antennen kann das Funksignal in eine spezifische Richtung verstärkt werden.

Reichweite

Die Reichweite der Funkverbindung wird von der Umgebung beeinflusst. Abhängig von der Bauart von Wänden wird das Funksignal unterschiedlich stark abgeschwächt. Feldtests haben ergeben, dass es durchaus möglich ist, mehrstöckige Gebäude vom Keller bis in den Dachstock per Funk zu vernetzen. Generell spricht man von Übertragungsdistanzen von 15 bis 40 Metern in Gebäuden und über 270 Metern bei Sichtkontakt. Dank neuster Technologien kann durch die Verkettung von bis zu sechs Access-Points eine flächendeckende Signalabdeckung realisiert werden.

Sicherheit

Verdient WLAN punkto Sicherheit seinen schlechten Ruf? Nicht die eigentliche WLAN-Technologie ist unsicher! Leider gehen die meisten Anwender sorglos damit um und verzichten auf vorhandene Sicherheitsmechanismen. Dies beginnt bei grundlegenden Einstellungen wie dem Ändern des Standardpassworts beim verwendeten Router. Ist dann die erste Verbindung gelungen, wird vor lauter Freude die Aktivierung der Sicherheitseinstellungen vergessen.
Netzwerke über Funk sind sicher - je besser alle Sicherheitsmechanismen ausgeschöpft werden.
Standardpasswort des Wireless-LAN-Routers umgehend ändern Verstecken des Access-Point-Namens (hide ESSID) Einschränken des Zugriffs auf WLAN-Access-Point auf bekannte Adapter. Jedes Gerät für ein Netzwerk (auch WLAN-Adapter) verfügt

über eine einmalige MAC-Adresse und kann so identifiziert werden. Erfassung der Adapter-MAC-Adressen im MAC-Adressfilter.
Aktivierung der WEP-Funktion (Wired-Equivalent-Privacy). Durch das Konfigurieren eines persönlichen Schlüssels auf dem Access-Point und dem Client wird die WEP-Funktion aktiviert, und alle Daten werden mit einer 64-bit- oder 128-bit-WEP-Verschlüsselung chiffriert.
Nutzung von 802.1x, wobei sich der Client mit einem persönlichen Benutzernamen und Passwort beim Access-Point anmelden kann.

Höhere Sicherheitsstufe bei Wireless-LAN
Noch höhere Sicherheit bietet der Einsatz von VPN (Virtual-Private-Networks) über das Wireless-LAN. Unabhängig von der Verbindung (drahtlos oder verkabelt) wird der Datenverkehr dabei verschlüsselt. Firmen sollten den Einsatz von VPN in Betracht ziehen, für Private sind die normalen Sicherheitsvorkehrungen meist ausreichend.